

Criado por:	Assunto	Versão	Data	Cod
Bruno Ricardo Pin	Regras Bitdefender	1	17/10/2022	MI069

Criação e geração de regras de modo geral e para cada departamento.

Política Sulplast:

Foi definida as seguintes regras:

Geral:

Notificações:

Mostrar ícone na área de notificação

Visibilidade de Problemas do Endpoint

Configurações:

Configurada senha de desinstalação: Conforme informação na planilha

Configuração de Proxy:

☒ Configuração de Proxy

Servidor: *	<input type="text" value="192.168.0.1"/>
Porta: *	<input type="text" value="3128"/>
Nome do usuário:	<input type="text" value="bluepex"/>
Senha:	<input type="password" value="....."/>


Power User: Conforme informação na planilha

Opções:

Opções


Remover eventos mais antigos do que (dias):

☒ Enviar relatórios de falhas para a Bitdefender

☒ Envie arquivos suspeitos para análise 

☒ Envie comentários sobre a saúde dos agentes de segurança

☒ Use a Rede Protetora Global da Bitdefender para aprimorar a proteção

☒ Permitir que os endpoints enviem dados de login do usuário para GravityZone 

Atualizações:


☒ Atualização do Produto

Recorrência:

Intervalo de Atualização (horas):

☒ Adiar reinicialização

☐ Se necessário, reiniciar após instalar atualizações a cada às :

☐ Atualize os módulos Linux EDR usando a atualização do produto 

Recorrência: De hora em hora

Intervalo de Atualização (horas): 1

Locais de Atualização ⓘ

Adicionar localização

Priorid...	Servidor
------------	----------

1	Servidores Relay
2	https://update-cloud.2d585.cdn.bitdefender.net

☒ Use o Servidor de Atualização Pública da Bitdefender como substituto

Círculo de Atualização

Circulo de

Atualização:

Slow Ring

Antimalware:
On-Access:
Normal
Na execução:

☒ Controle avançado de ameaças (ATC)

Ação padrão para aplicativos infectados: Desinfectar

- ☐ - Agressivo
- ☒ - Normal
- ☐ - Permissivo

Normal - Recomendado para a maioria dos sistemas

Esta opção estabelecerá a taxa de detecção de Bitdefender Advanced Threat Control no nível médio, mostrando alertas que podem incluir alguns alarmes falsos (aplicativos limpos detectados como maliciosos).

☒ Proteção contra ataque sem arquivo

Quando ativada, essa opção permite que o GravityZone descubra e bloqueie automaticamente ataques sem arquivos no estágio de pré-execução.

☒ Scanner de linha de comando

☐ Provedor de segurança da interface de verificação antimalware

☐ Relatar os resultados da análise para a Interface de Verificação Antimalware

✓ Mitigação de Ransomware

Recupere arquivos criptografados por ransomware, assim que os módulos de proteção GravityZone detectarem e bloquearem o ataque.

Monitor:

- ☒ **Localmente**
Monitora os processos executados localmente no terminal. É recomendado para estações de trabalho. Use com cuidado em servidores devido ao impacto no desempenho.
- ☒ **Remoto**
Monitora os caminhos de compartilhamento de rede acessados remotamente. Use esta opção se o ponto de extremidade for um servidor de arquivos ou se os compartilhamentos de rede estiverem ativados.

Recuperar:

☒ **Sob solicitação**
O GravityZone recupera os arquivos somente quando você escolhe na página de Atividade do Ransomware.

☐ **Automaticamente**
GravityZone recupera os arquivos automaticamente após a detecção de um ransomware.

Rastreamento Completo:

[Geral](#) [Opções](#) [Alvo](#)

Detalhes

Nome da Tarefa:

Rastreamento Completo

- ☒ Executar a tarefa com prioridade Baixa
- ☐ Desligar o computador quando a análise terminar

Agendador

Data e hora de início:

02/04/2016

12

:

00

Recorrência

- ☐ Agendar tarefa para executar todo: 1 dia(s)
- ☒ Executar tarefa todo: ☐ Dom ☐ Seg ☒ Ter ☐ Qua ☐ Qui ☒ Sex ☐ Sáb

- ☒ Se o horário de execução agendado for perdido, executar tarefa assim que possível

- ☐ Pular se a próxima tarefa agendada iniciar em menos de

1

dia(s)

Configurações da Varredura

Verificação Contextual

Defina as configurações para a verificação de arquivos e pastas no ponto de extremidade local no menu contextual do Windows Explorer. Você pode escolher um perfil de verificação predefinido ou personalizar as configurações de verificação contextual, como o tipo de ameaças a serem verificadas ou a ação a ser executada, cada tipo de detecção.

Varredura de Dispositivos Externos

Configure as opções de varredura para os dispositivos externos especificados. Você pode escolher um perfil de varredura predefinido ou personalizar as configurações de varredura do dispositivo, como os tipos de arquivos a serem verificados ou a ação a ser executada em cada tipo de detecção.

☒ Análise de Dispositivos

- ☒ Mídia de CD/DVD
- ☒ Dispositivos de armazenamento USB
- ☐ Não analisar dispositivos com mais de (MB) de dados armazenados 0

Deteção antiexploit avançado:

Detecções do sistema amplo

Detecções de Windows

- ☒ Escalação de privilégio Cancelar Processo
- ☒ LSASS protection Block Only

Detecções de Linux

- ☒ Monitoramento de credenciais Somente Reportado
- ☒ Monitoramento PTrace Somente Reportado
- ☒ Monitoramento de namespace Somente Reportado
- ☒ Monitoramento de corrupção Somente Reportado
- ☒ Monitoramento SUID Somente Reportado

Configurações:

Quarentena

Apagar arquivos mais antigos que (dias):

30

☒ Enviar arquivos em quarentena ao Bitdefender Labs a cada (horas)

1

☒ Revise a quarentena após atualizações de conteúdo de segurança de malware

☒ Copiar arquivos para quarentena antes de aplicar a ação de desinfecção

☒ Permitir que os usuários tomem ações em quarentena local

☒ In-policy exclusions

Firewall:

Geral:

☒ Firewall

☐ Permitir Compartilhamento de Conexão com a Internet (ICS)

☒ Monitorar Conexões Wi-Fi

☒ Registrar nível de verbosidade

Baixa

☒ Bloquear análise de portas

☐ Exclusões

Políticas:

Configurações

Nível de Proteção:

Definir regras, arquivos conhecidos e permitir

☐ Criar regras agressivas

☒ Criar regras para aplicativos bloqueados por IDS

☒ Monitorar alterações de processos

☒ Ignorar processos assinados

Políticas

+ Adicionar Para cima Abaixo Exportar Importar Apagar

	Priori...	Nome	Tipo de regra	Rede	Protocolo	Permissão
<input type="checkbox"/>	1	Entrada de ICMP	Aplicativo	Casa / Escritóri...	ICMP	Permitir
<input type="checkbox"/>	2	Entrada de ICMPv6	Aplicativo	Casa / Escritóri...	IPv6-ICMP	Permitir
<input type="checkbox"/>	3	Entrada de Conexões Remotas ao Desktop	Conexão	Casa / Escritóri...	TCP	Permitir
<input type="checkbox"/>	4	Envio de e-mails	Conexão	Casa / Escritóri...	TCP	Permitir
<input type="checkbox"/>	5	Navegação na Rede HTTP	Aplicativo	Casa / Escritóri...	TCP	Permitir
<input type="checkbox"/>	6	Impressão de Rede	Aplicativo	Casa / Escritóri...	Qualquer	Permitir
<input type="checkbox"/>	7	Tráfego do Windows Explorer em FTP	Aplicativo	Casa / Escritóri...	TCP	Negar
<input type="checkbox"/>	8	Tráfego do Windows Explorer em HTTP	Aplicativo	Casa / Escritóri...	TCP	Negar









Geral:

☒ Proteção de rede

Ao desativar este módulo, você desativará todos os seus recursos e não poderá modificar nenhuma configuração.

Configurações Gerais

☒ Analisar SSL☒ Analisar HTTP☐ Verificar RDP☐ Mostrar barra de ferramentas do navegador (legado)☐ Orientador de pesquisa do navegador (legado)☒ Exclusões 

IP/mask	Entidade	Observações	
Tipo	Entidade Excluída	Observações	Ação
IP	192.168.0.201	DelsoftPRD	
IP	192.168.0.249	DelsoftTST	
URL	*sulplast.com.br*	Site Sulplast	
IP	192.168.0.204	AIMS	
IP	192.168.0.219	GLPI	
IP	192.168.0.252	Vedois	
IP	192.168.0.220	GLPI-TESTE	
IP	192.168.0.251	Rocket.Chat	

Primeira Página ← Página 1 de 1 → Última Página 20

8 items

Proteção na Web:

☒ Antiphishing

Ação padrão para alvos suspeitos:

Bloquear

☒ Proteção contra fraudes☒ Proteção contra phishing☒ Verificação de tráfego na Web

Verifica todo o tráfego HTTP de entrada em tempo real, para detectar e bloquear o download de cargas maliciosas em seu ambiente.

☒ Verificação de tráfego de e-mail☒ E-mails recebidos (POP3)☒ E-mails enviados (SMTP)

Ataques de rede:

☒ Defesa de Ataque em Rede

Esse recurso é uma camada de segurança projetada para detectar técnicas de ataque à rede que tentam obter acesso a pontos de extremidade específicos. Pode ser personalizado para atender aos requisitos de segurança da sua organização.

Técnicas ATT&CK

<input checked="" type="checkbox"/>	Acesso Inicial	Bloquear
<input checked="" type="checkbox"/>	Acesso à credencial	Bloquear
<input checked="" type="checkbox"/>	Descoberta	Bloquear
<input checked="" type="checkbox"/>	Movimento lateral	Bloquear
<input checked="" type="checkbox"/>	Crimeware	Bloquear

[Restaurar ao padrão](#)

Controle de Dispositivos:**Políticas:**

Apenas o Windows Portable e Armazenamento Externo são bloqueados;

Exclusões:

Quando houver necessidade informar na lista qual dispositivo deverá ficar fora da regra.

Gerenciamento de riscos:☒ **Gerenciamento de riscos**

Permite uma varredura de risco recorrente nos terminais de destino. Isso significa que você pode agendar a verificação de riscos à segurança, como atualizações automáticas ou configurações de controle de acesso do usuário. Use as seguintes opções para definir o agendamento da varredura de riscos para os terminais de destino.

[Leia a descrição completa dos indicadores de risco e as ações de correção disponíveis.](#)

Agendador

Data e hora de início:

05/10/2021

10

:

30

Recorrência

Agendar tarefa para executar todo:

1

dia(s)



Executar tarefa todo:



Dom



Seg



Ter



Qua



Qui



Sex



Sáb



Se o horário de execução agendado for perdido, executar tarefa assim que possível